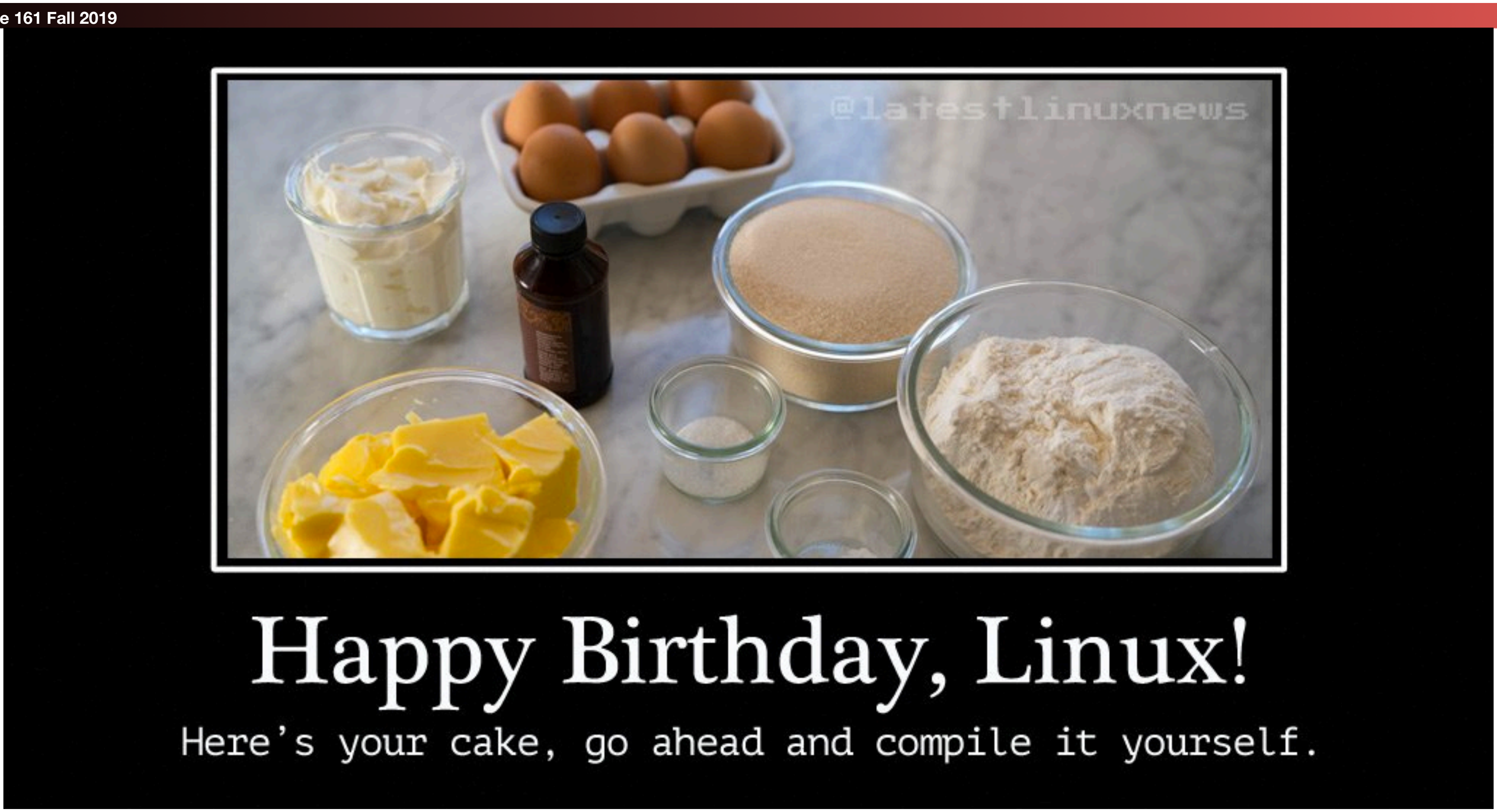
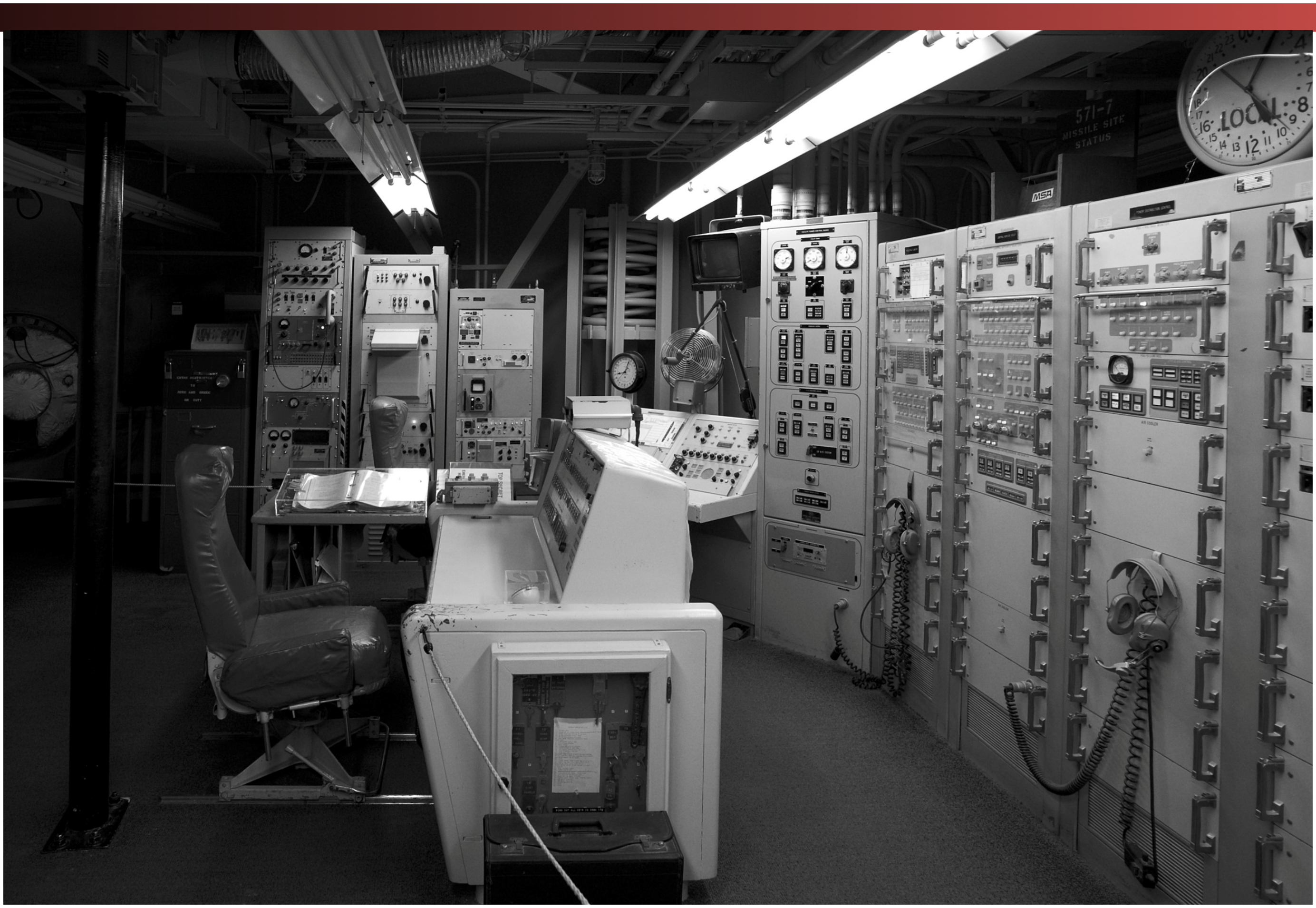

@latestlinuxnews
Happy Birthday, Linux!
Here's your cake, go ahead and compile it yourself.

Security Principles

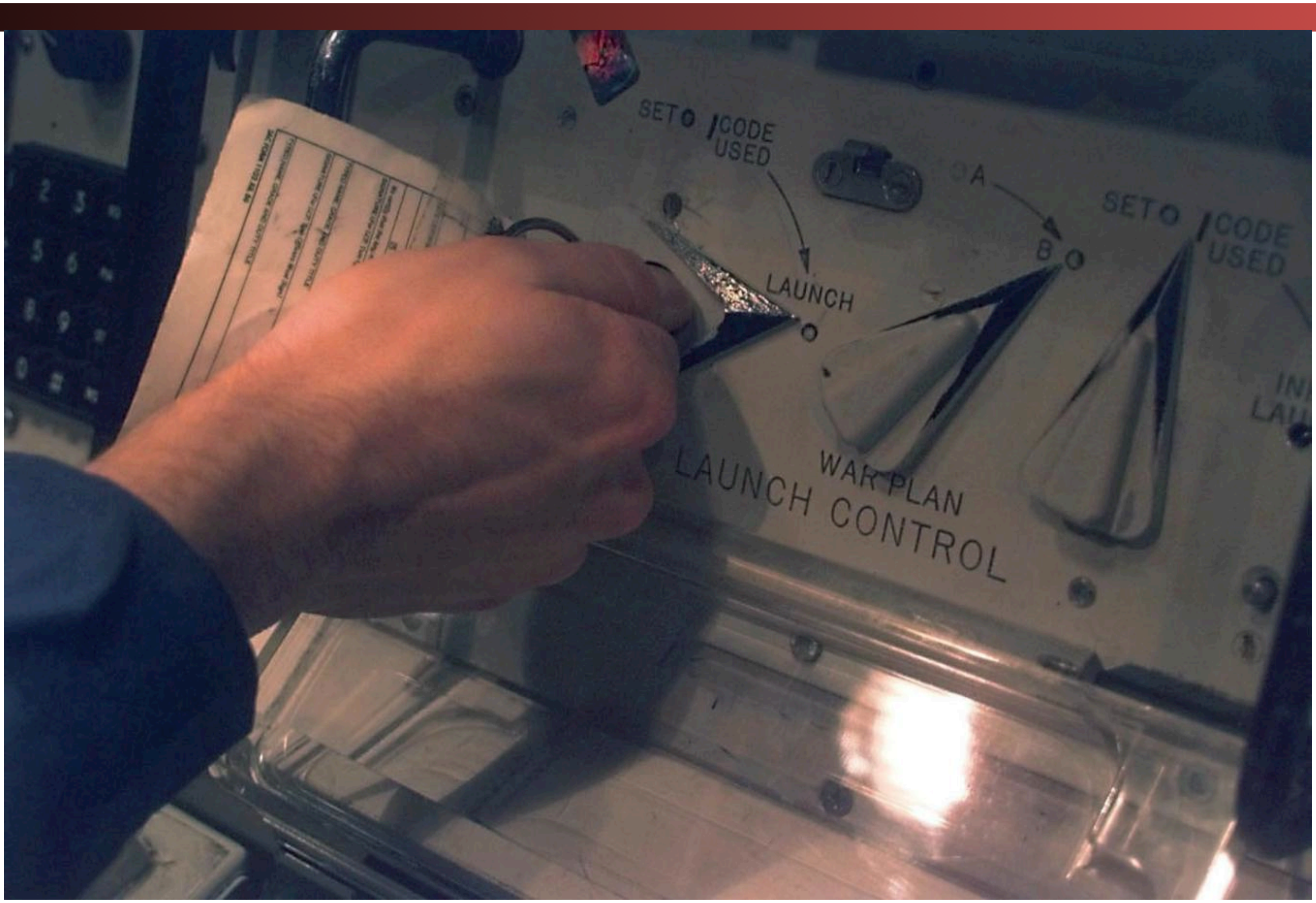
Administrivia...

- Discussion and office hours start this week
  - Go to any section you want that isn't full:
    See the course webpage for the calendar
- Homework 1 released
  - Due in ~1.5 weeks, on Gradescope
- Exam conflicts
  - Private post in "Accommodations" on Piazza:
    Make-up exam will be ***immediately*** after the scheduled exam time (so 9-11pm)

Welcome to a Nuclear Bunker

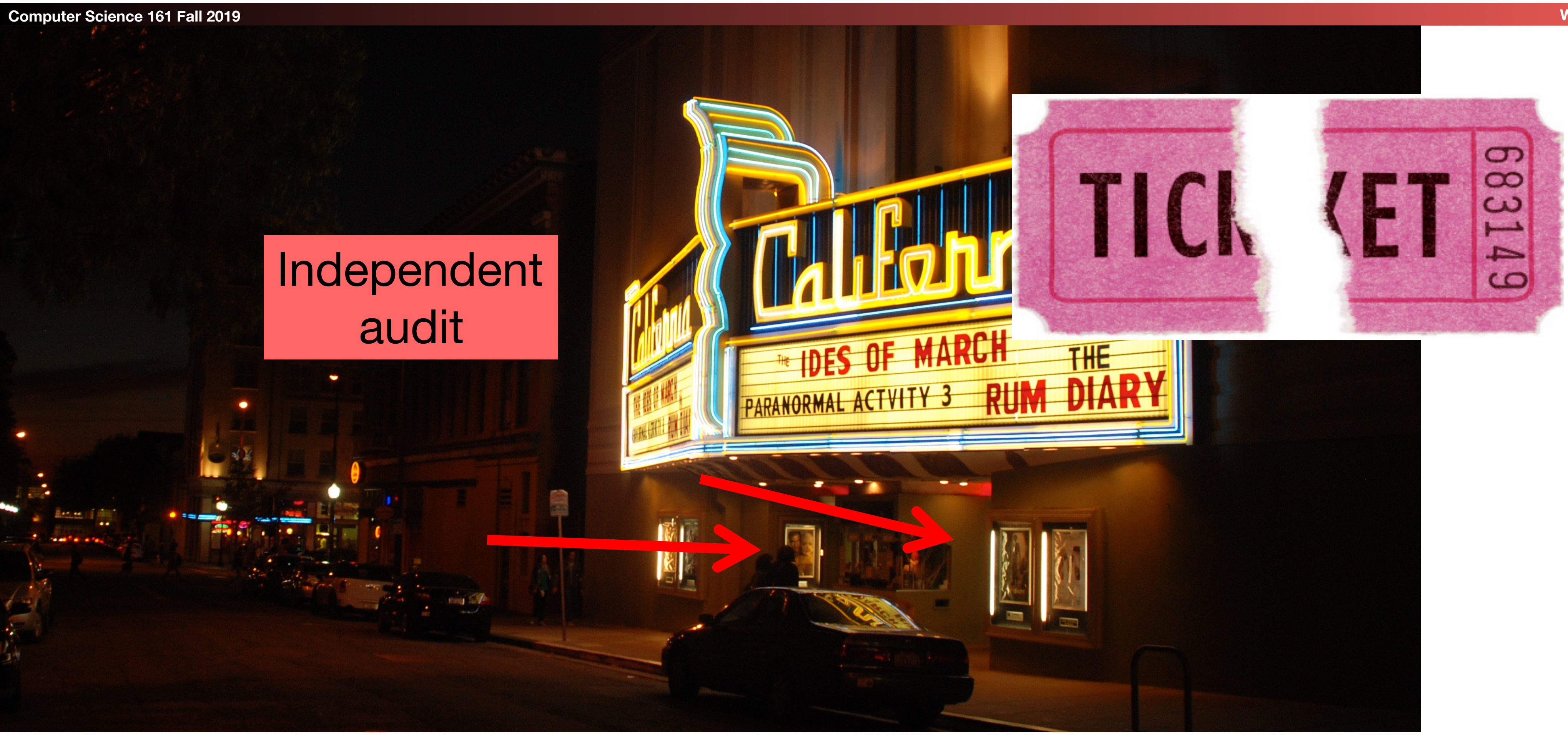


Two Man Control:
Each Needs To Turn the Key



Desired Security Property:
Only Want To Destroy The World On Purpose

“Separation of responsibility.”

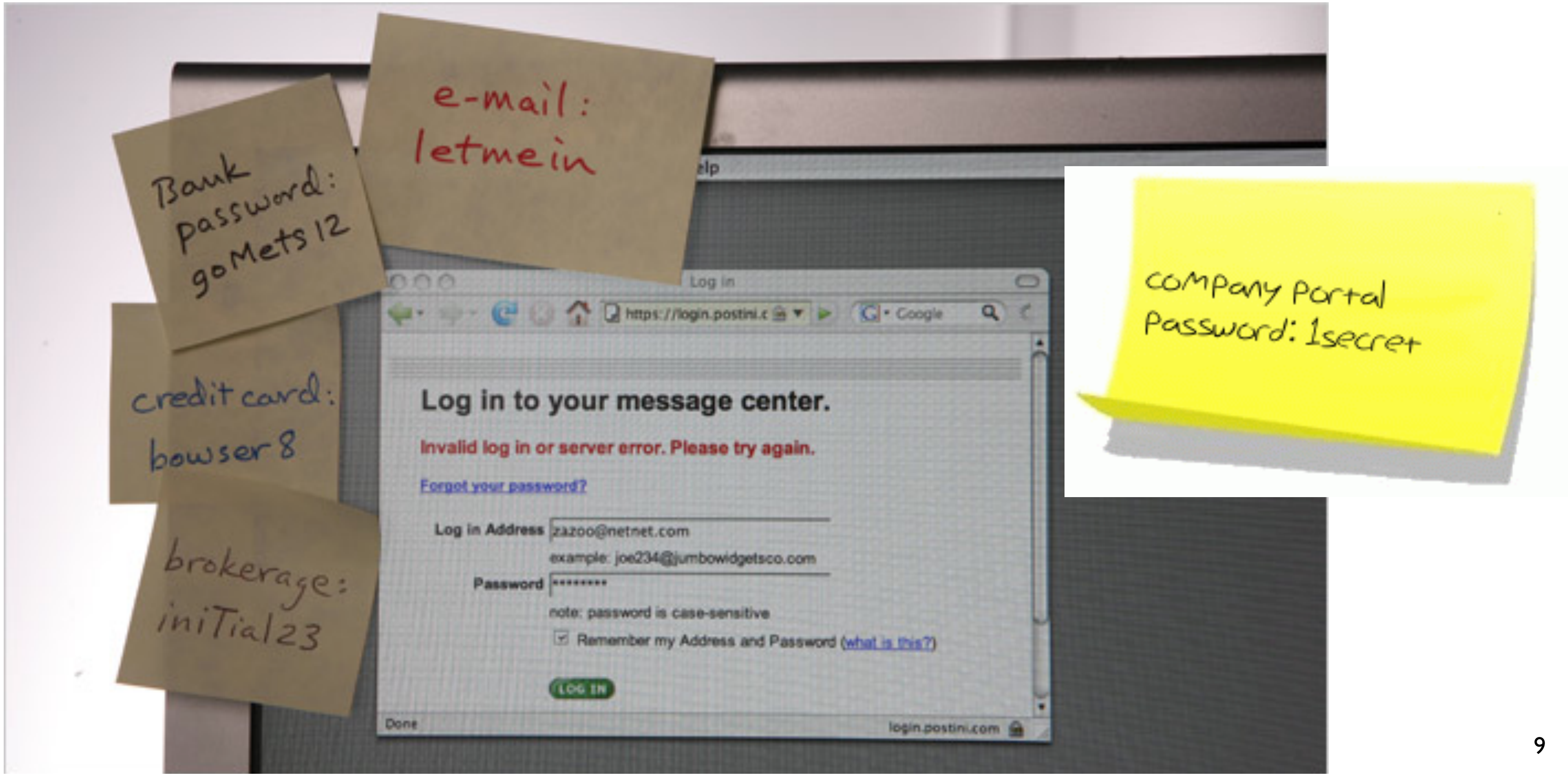


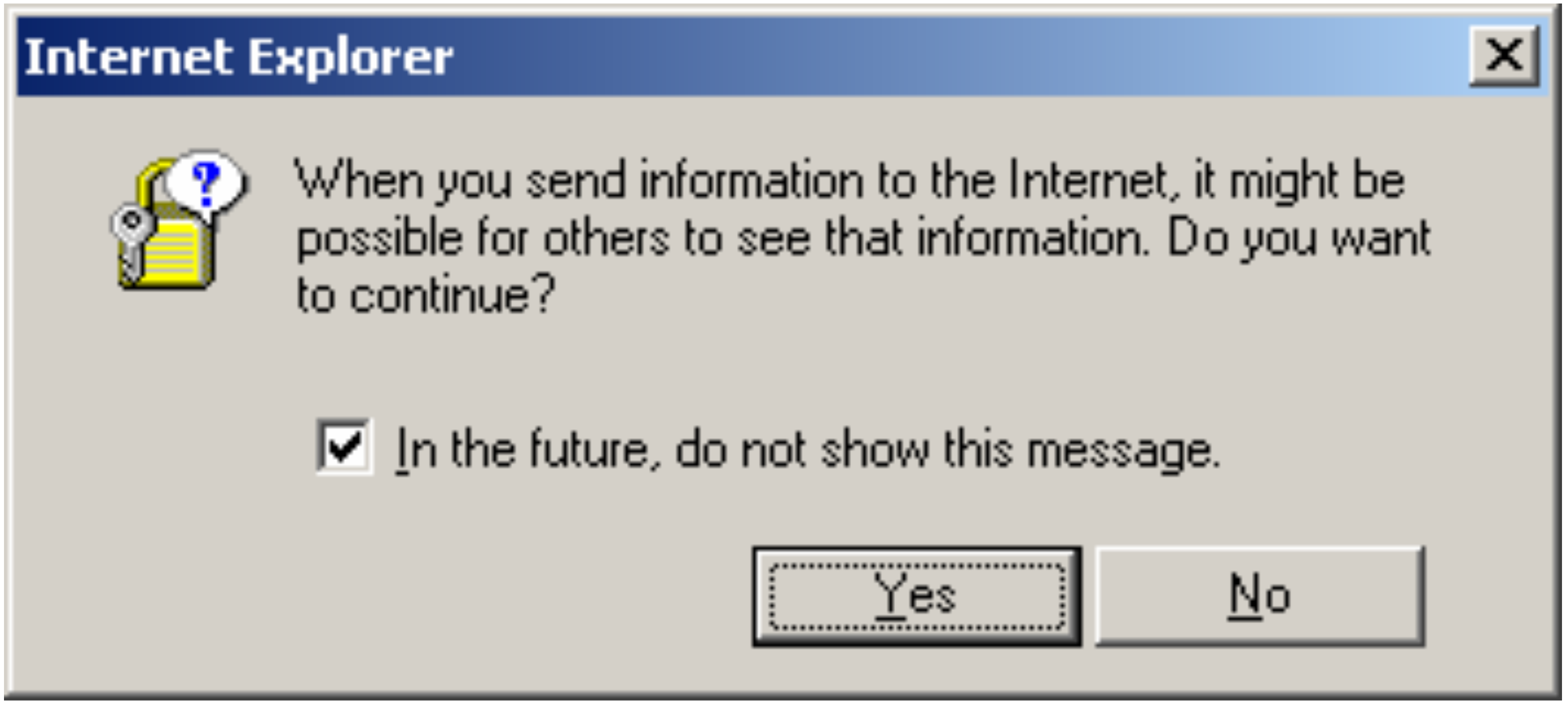
Independent audit

Summary:
Notions Regarding Managing Privilege

- Least privilege
  - The notion of avoiding having unnecessary privileges
- Privilege separation
  - A way to achieve least privilege by isolating access to privileges to a small Trusted Computing Base (TCB)
- Separation of responsibility
  - If you need to have a privilege, consider requiring multiple parties to work together (collude) to exercise it

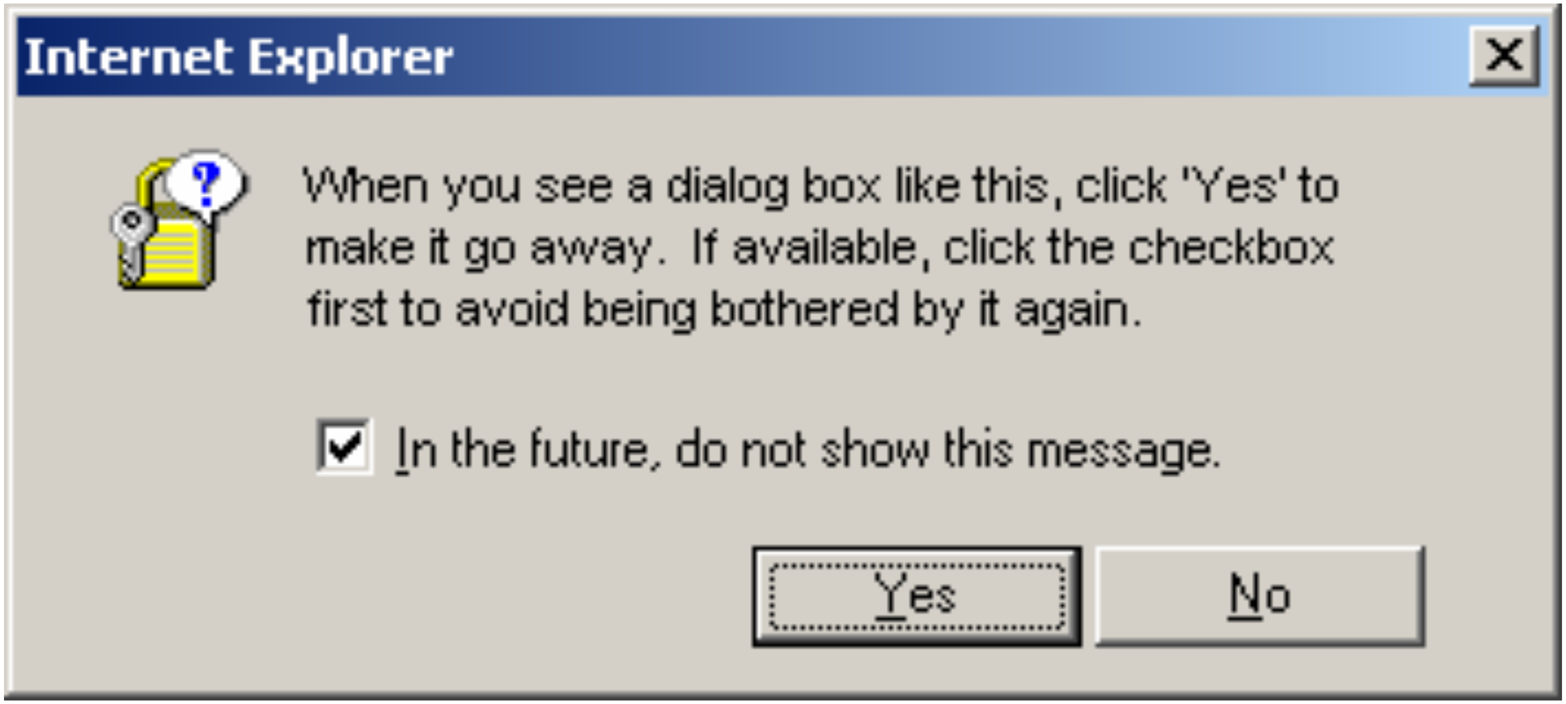
Impact of a Password Policy


Bank password: goMets12
e-mail: letmein
credit card: bowser8
brokerage: iniTial23
company Portal Password: 1secret
Log in
https://login.postini.c
Google
Log in to your message center.
Invalid log in or server error. Please try again.
Forgot your password?
Log in Address zazoo@netnet.com
example: joe234@jumbowidgetsco.com
Password *********
note: password is case-sensitive
☑ Remember my Address and Password (what is this?)
LOG IN
Done
login.postini.com



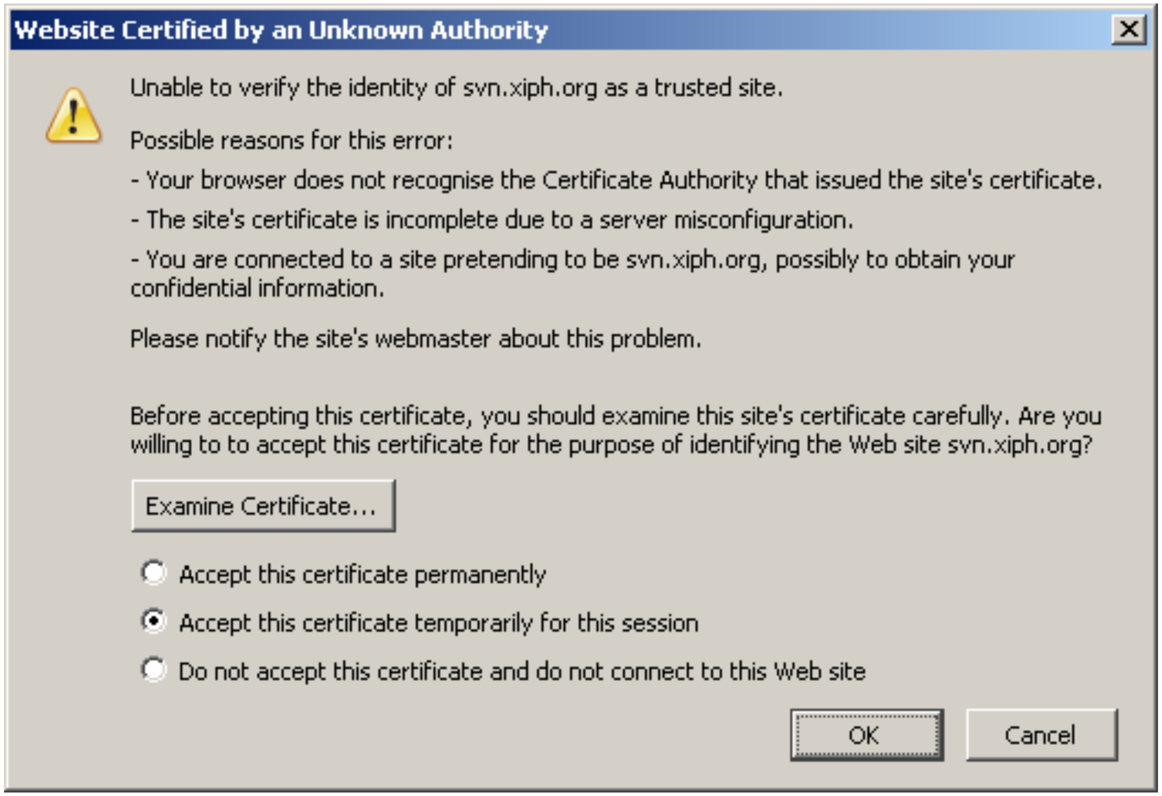
When you send information to the Internet, it might be possible for others to see that information. Do you want to continue?

☑ In the future, do not show this message.



When you see a dialog box like this, click 'Yes' to make it go away. If available, click the checkbox first to avoid being bothered by it again.

☑ In the future, do not show this message.



Unable to verify the identity of svn.xiph.org as a trusted site.

Possible reasons for this error:

- Your browser does not recognise the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be svn.xiph.org, possibly to obtain your confidential information.

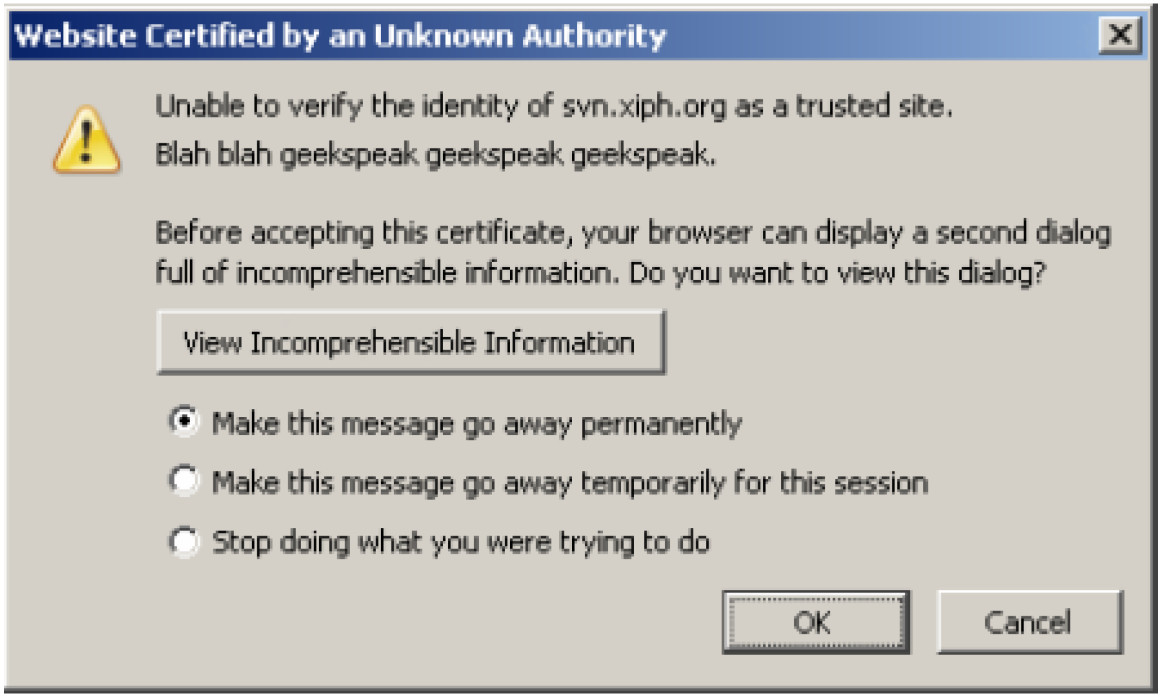
Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site svn.xiph.org?

○ Accept this certificate permanently

● Accept this certificate temporarily for this session

○ Do not accept this certificate and do not connect to this Web site



Website Certified by an Unknown Authority

Unable to verify the identity of svn.xiph.org as a trusted site.
Blah blah geekspeak geekspeak geekspeak.

Before accepting this certificate, your browser can display a second dialog full of incomprehensible information. Do you want to view this dialog?

● Make this message go away permanently

○ Make this message go away temporarily for this session

○ Stop doing what you were trying to do

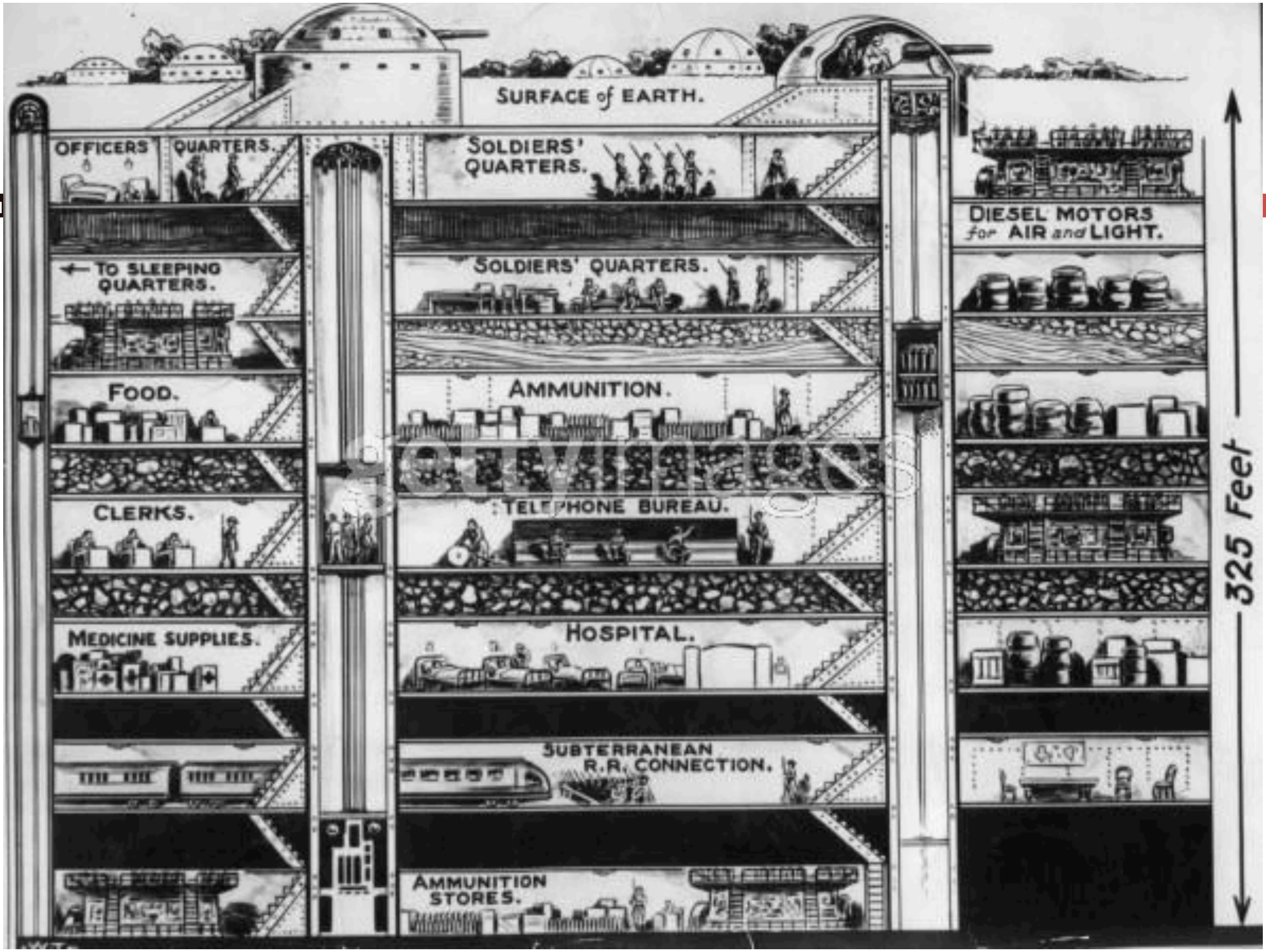
Security Keys and Human Factors

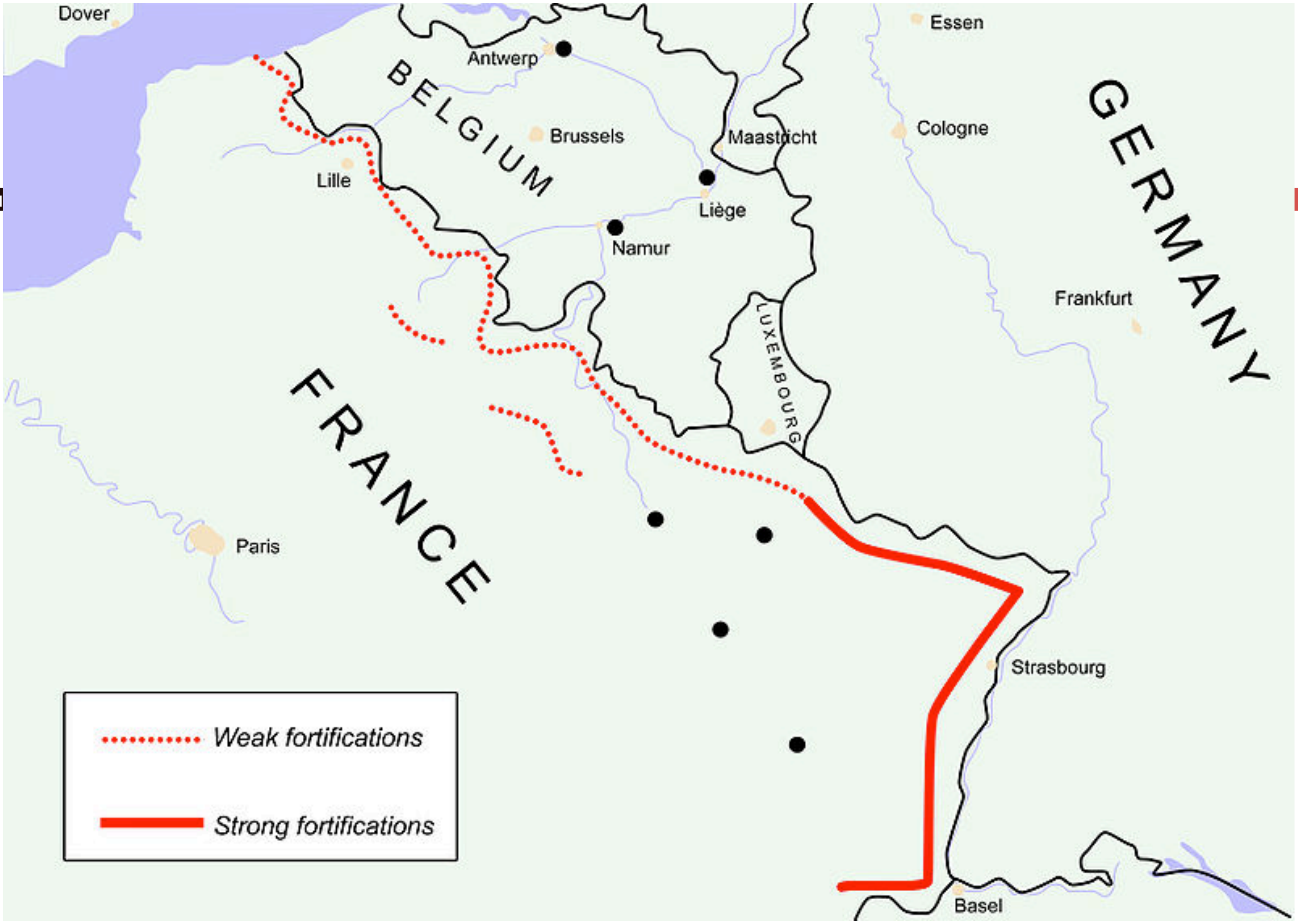
- This is a security key for storing key material for an encrypted military phone
  - Leverages a lifetime of knowledge in how to protect physical keys
- U2F security keys leverage the same knowledge!
- Product/design idea:
  A ***physical*** doorlock that uses a U2F key!

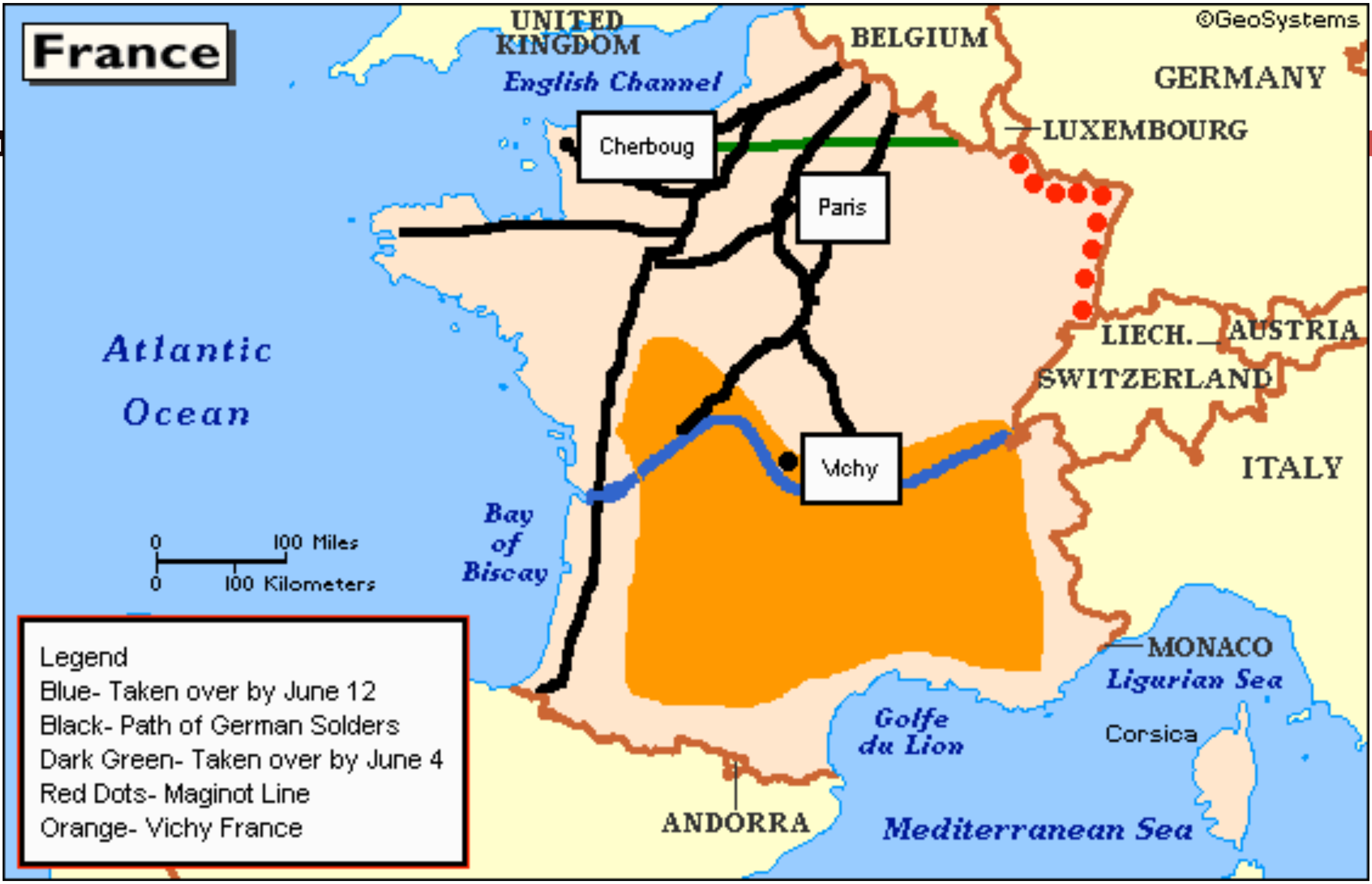
Summary:
Dealing with Users

- Psychological acceptability
  - Will users abide a security mechanism, or decide to subvert it?
    - Remember Rule 777...
- Consider human factors
  - Does a security mechanism assume something about human behavior when interacting with the system that might not hold, even in the absence of conscious decisions by the users to subvert
  - Have the computer do computer-y things, and humans do human-y things

2


SURFACE of EARTH.
OFFICERS' QUARTERS.
SOLDIERS' QUARTERS.
DIESEL MOTORS for AIR and LIGHT.
← TO SLEEPING QUARTERS.
SOLDIERS' QUARTERS.
FOOD.
AMMUNITION.
CLERKS.
TELEPHONE BUREAU.
MEDICINE SUPPLIES.
HOSPITAL.
SUBTERRANEAN R.R. CONNECTION.
AMMUNITION STORES.
325 Feet


Dover
Antwerp
BELGIUM
Brussels
Maastricht
Essen
Cologne
GERMANY
Lille
Liège
Namur
Frankfurt
LUXEMBOURG
FRANCE
Paris
Strasbourg
Basel
Weak fortifications
Strong fortifications

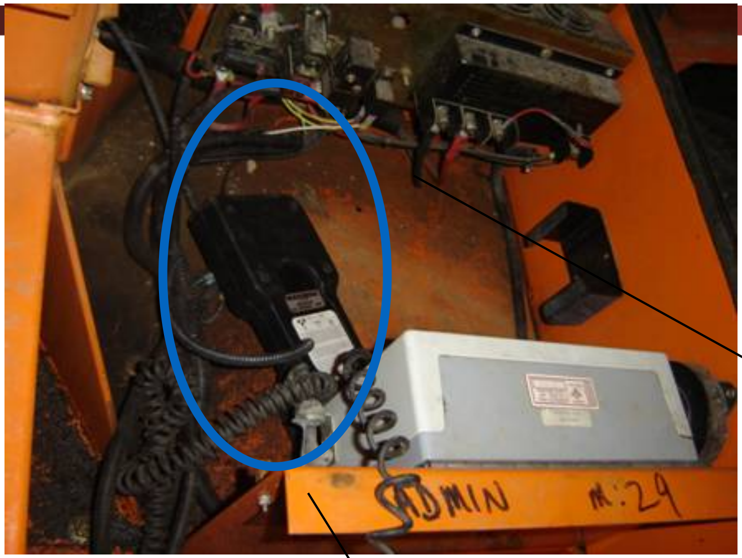

France
©GeoSystems
UNITED KINGDOM
English Channel
BELGIUM
GERMANY
LUXEMBOURG
Cherboug
Paris
Vichy
LIECH.
AUSTRIA
SWITZERLAND
ITALY
Atlantic Ocean
Bay of Biscay
0 100 Miles
0 100 Kilometers
MONACO
Ligurian Sea
Corsica
Golfe du Lion
ANDORRA
Mediterranean Sea
Legend
Blue- Taken over by June 12
Black- Path of German Solders
Dark Green- Taken over by June 4
Red Dots- Maginot Line
Orange- Vichy France

“Only as secure as the weakest link.”

- "A door lock is only as strong as the window"

ACCIDENT
ON
MOTORWAY

ACCIDENT
ON
MOTORWAY


ADMIN
M:29

F1
NO
YES

CAUTION!
ZOMBIES!
AHEAD!!!
RUN FOR
COLD
CLIMATES
THE END
IS NEAR!
!!!!!!!!
NAZI
ZOMBIES!
RUN!!!

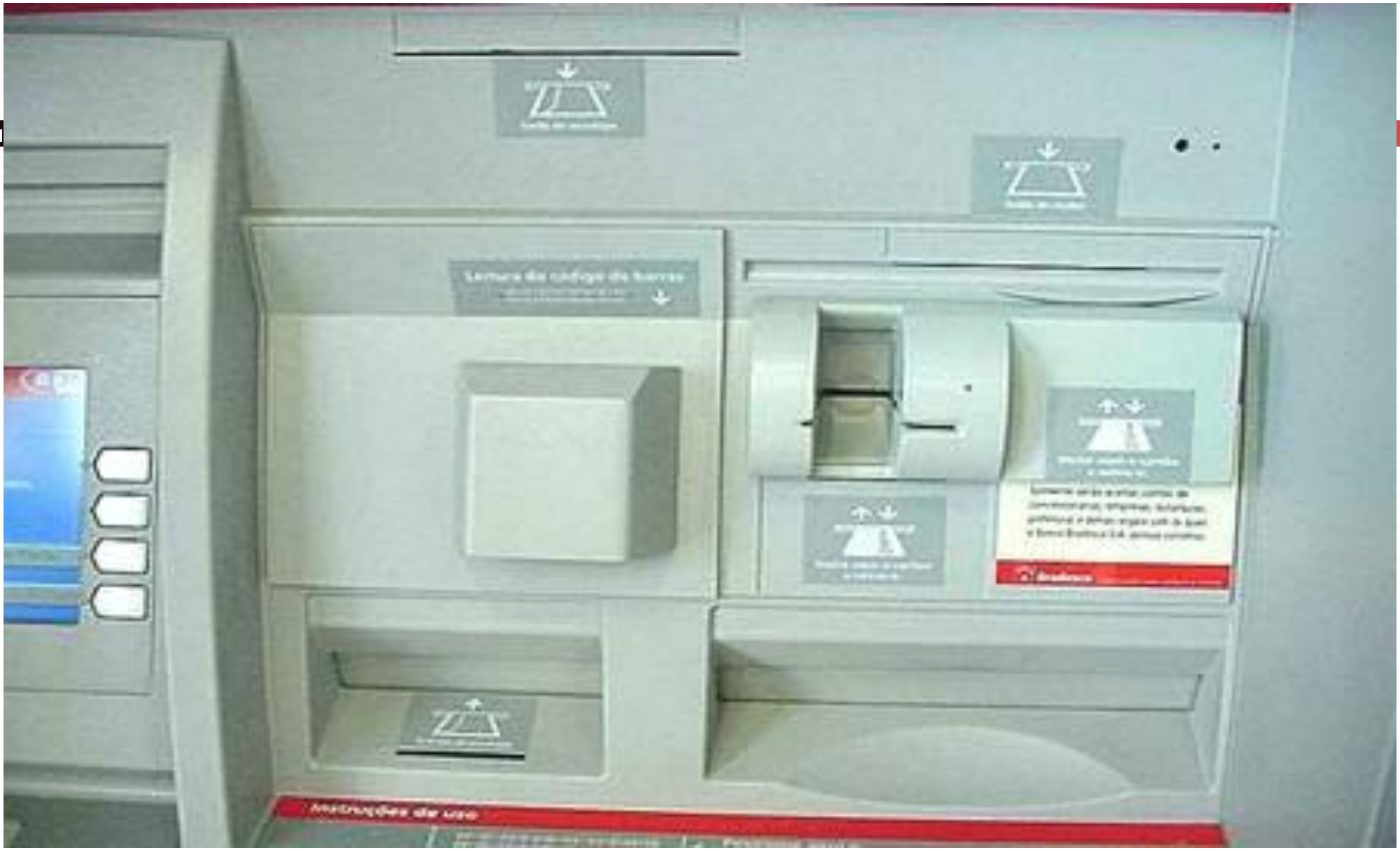
RAPTORS
AHEAD
CAUTION

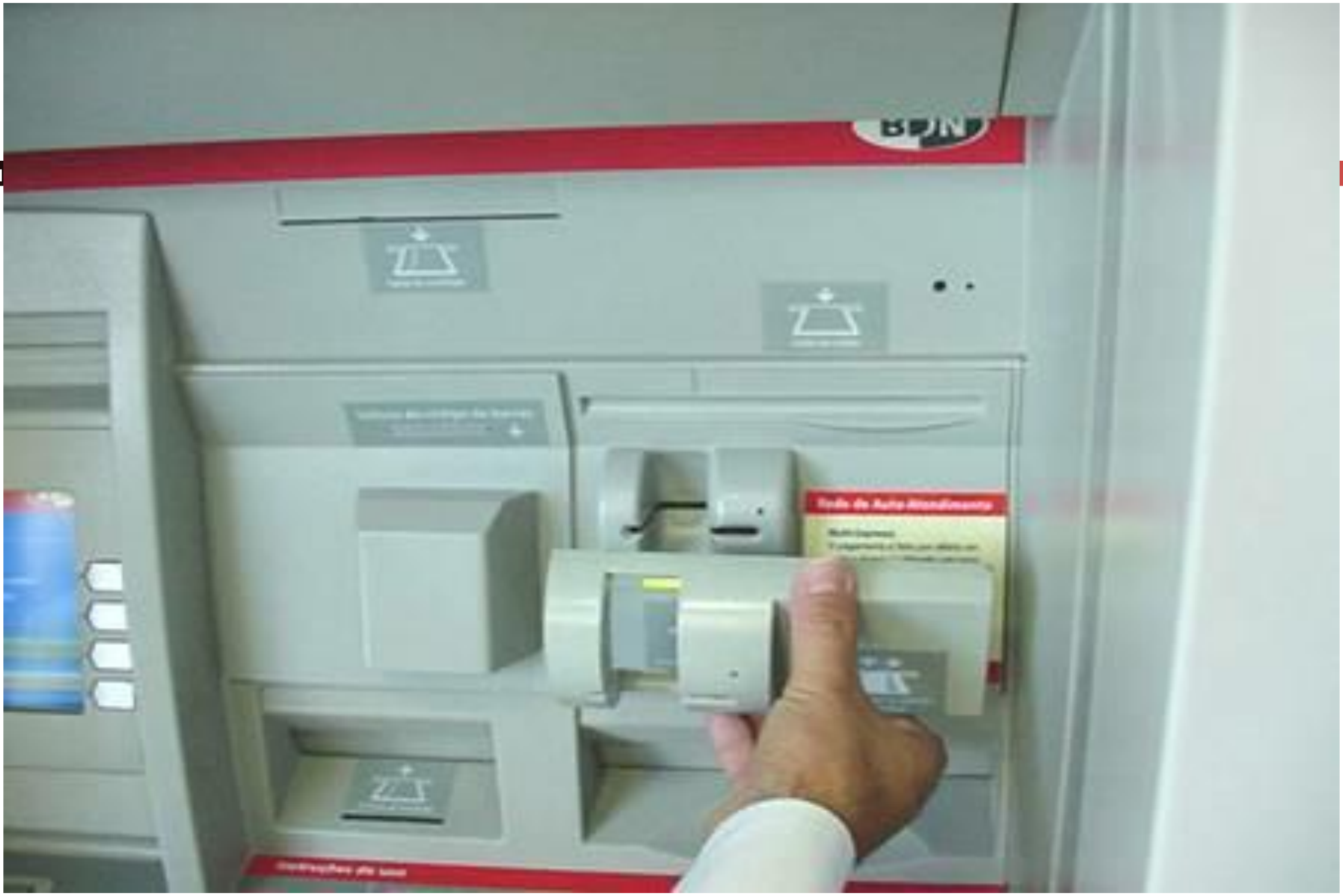
TRAPPED
IN SIGN
FACTORY

SEND
HELP!

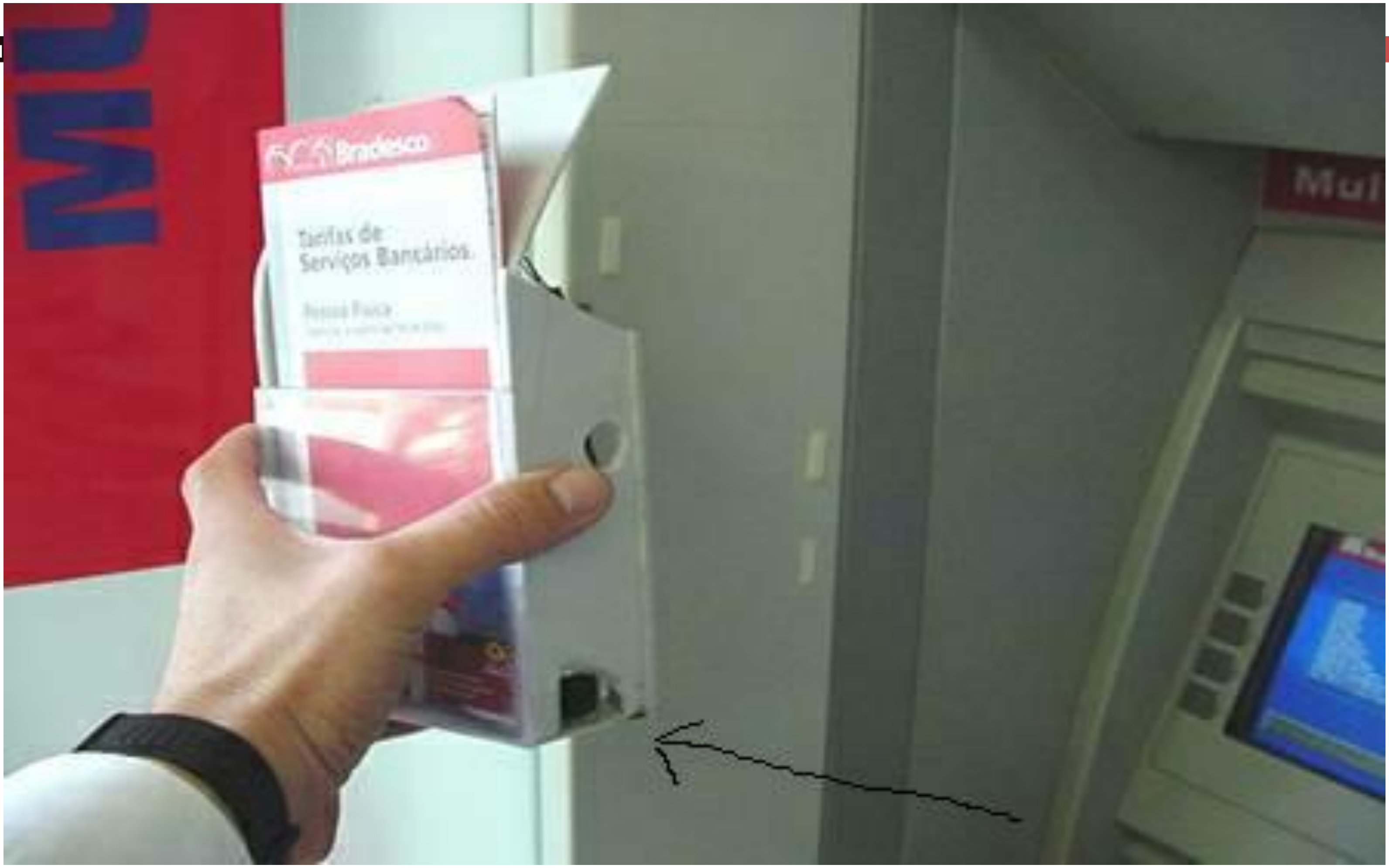
“Don’t rely on security through obscurity.”

- Because otherwise the raptors will get you...
- Obscurity does help but you need to design your system so that it fails...
- Kerckhoffs's Principle:
  - A cryptosystem should be secure even if everything about the system, ***except the key***, is public knowledge.
- Shannon's Maxim:
  - The enemy knows the system

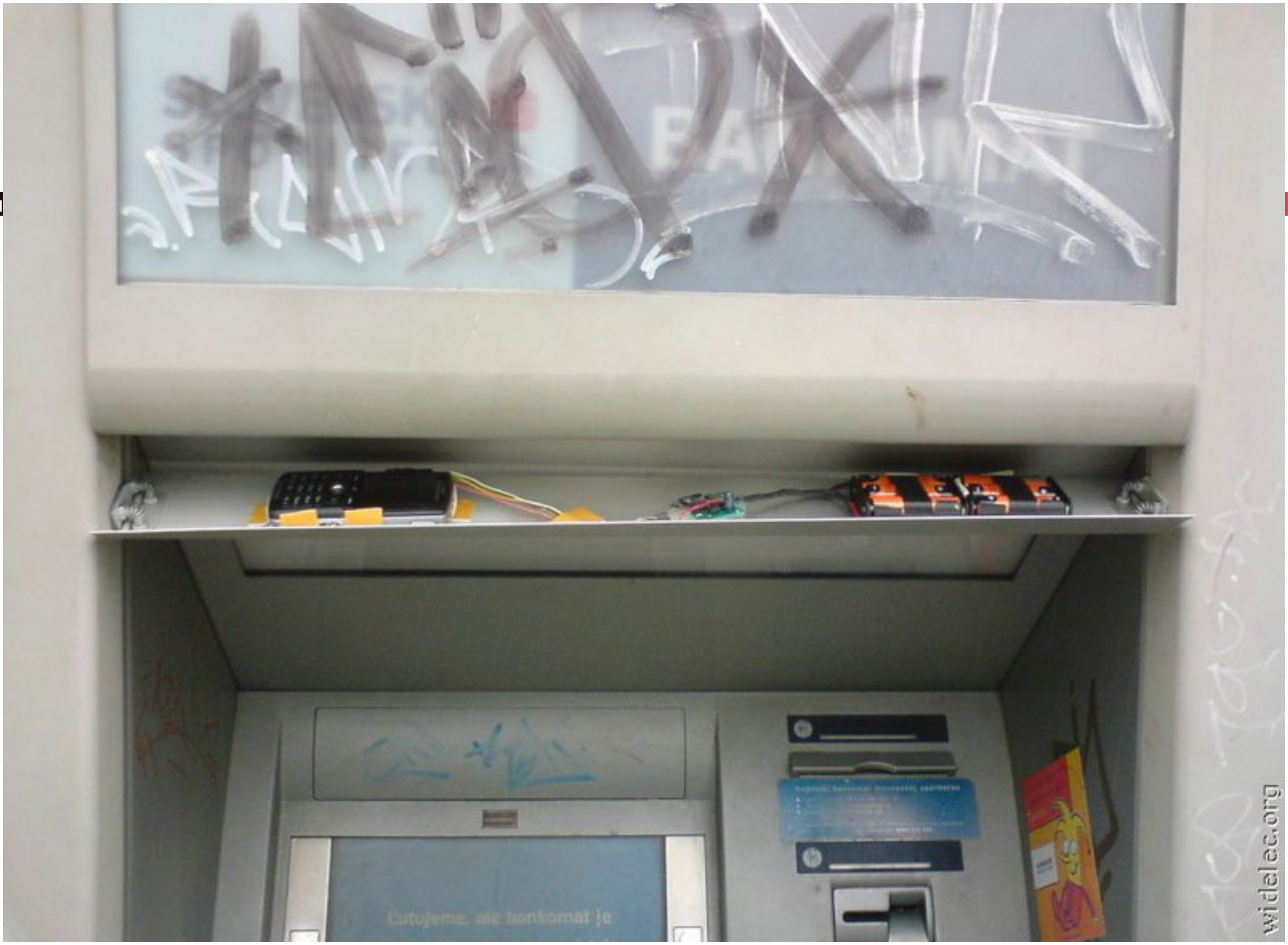

Leitura de código de barras
Instruções de uso



Bradesco
Tarifas de Serviços Bancários
Pessoa Física
Multi Expresso
Bradesco


MU
Bradesco
Tarifas de
Serviços Bancários.
Pessoa Física
Mul

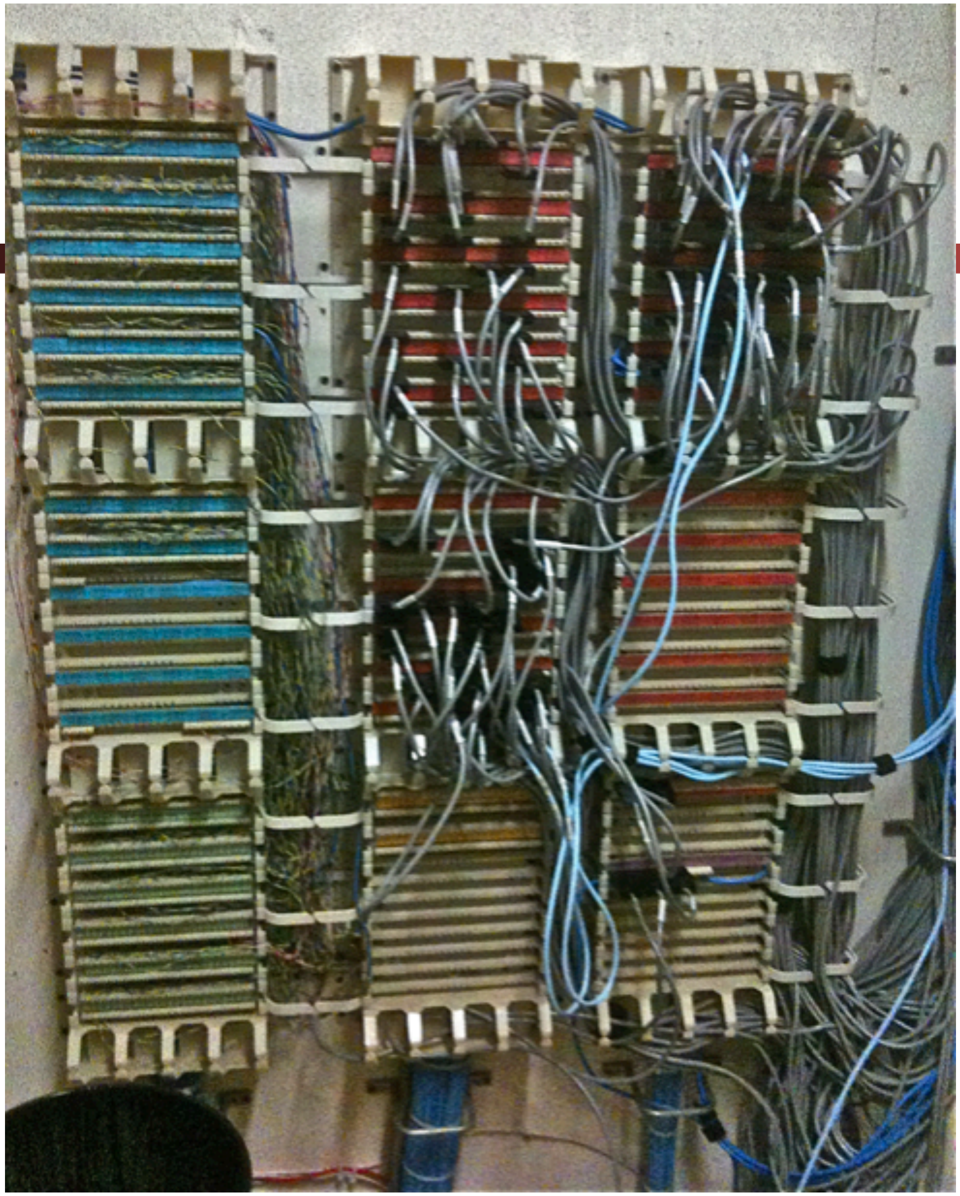
widelec.org
We regret this ATM
is temporarily out of service

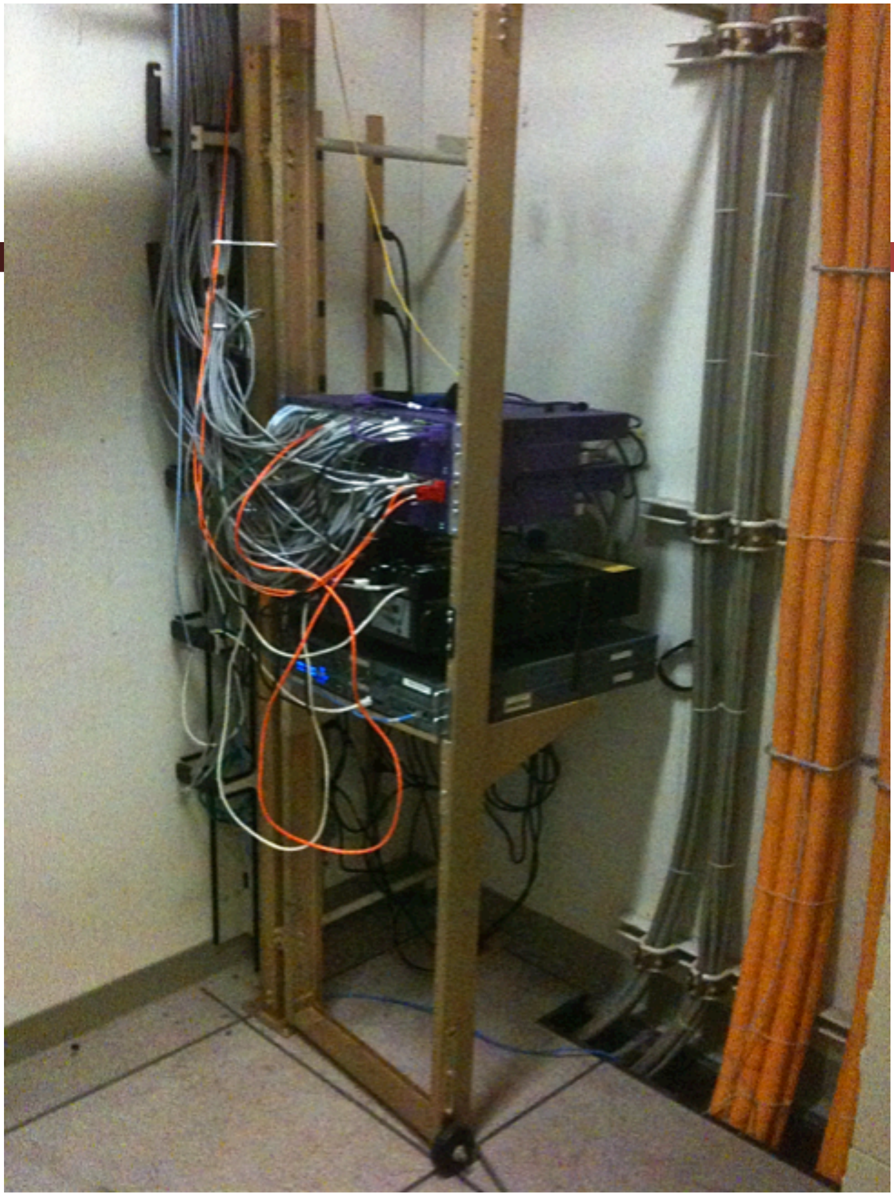

widelec.org
Čutujeme, ale bankomat je

“Trusted path.”

- Users need to know they are talking with the legit system
- System needs to know its talking with the legit user
- These channels need to be unspoofable and private
  - ATM skimmers are a failure of the trusted path

Soda Hall wiring closet





Protection?

398
COMMUNICATION

“Use fail-safe defaults.”

- But it can often be hard to determine
- Default for access here is reasonable...
  - Deny all except for an allowed user list
- But when the power goes out...
  - Should the lock fail shut?
    Should the lock fail open?

Common Assumptions When Discussing Attacks

- (Note, these tend to be pessimistic … but prudent)
- Attackers can interact with our systems ***without particular notice***
  - Probing (poking at systems) may go unnoticed …
  - … even if highly repetitive, leading to crashes, and easy to detect
- It’s easy for attackers to know general information about their targets
  - OS types, software versions, usernames, server ports, IP addresses, usual patterns of activity, administrative procedures

Common Assumptions, con't

- Attackers can obtain access to a copy of a given system to measure and/or determine how it works
    - Shannon's Maxim: "The Enemy Knows the System"
- Attackers can make energetic use of automation
    - They can often find clever ways to automate
- Attackers can pull off complicated coordination across a bunch of different elements/systems
- Attackers can bring large resources to bear if req'd
    - Computation, network capacity
    - But they are not super-powerful (e.g., control entire ISPs)

Common Assumptions, con’t

- If it helps the attacker in some way, ***assume they can obtain privileges***
  - But if the privilege gives everything away (attack becomes trivial), then we care about unprivileged attacks
- The ability to robustly detect that an attack has occurred ***does not replace desirability of preventing***
- Infrastructure machines/systems are well protected (hard to directly take over)
  - So a vulnerability that requires infrastructure compromise is less worrisome than same vulnerability that doesn’t

Common Assumptions, con’t

- Network routing is hard to alter … other than with physical access near clients (e.g., “wifi/coffeeshop”)
  - Such access helps fool clients to send to wrong place
  - Can enable Man-in-the-Middle (MITM) attacks
- We worry about attackers who are lucky
  - Since often automation/repetition can help “make luck”:
    If its 1 in a million, just try a million times!
- Just because a system does not have apparent value,
  it may still be a target
  - "Lets break into the Casino network... Through the fishtank"
- Attackers are mostly undaunted by fear of getting caught
  - There are exceptions

Patches & 0-days

- Systems have vulnerabilities all the time...
  - A ***patch*** is an update which is designed to remove such vulnerabilities.
- An "0-day" is an exploit where nobody but the attacker knows about
  - So there ***is*** no patch
- But 0-days are rare: Require independent discovery...
  - But it is straightforward to take a patch and find an exploit
- So patch religiously!
  - Similarly, the "patch" for influenza is the flu-shot. GET ONE!

And Most Exploits These Days Are Chains...

- EG, to pwn an iPhone...
  - Need an exploit for the browser to start running code within the browser's sandbox
  - And another exploit to break out of the sandbox and take over the OS kernel...
    - And that other exploit may actually be 2-3 exploits themselves chained together
- So e.g. on the massive Chinese campaign...
  - There was one known 0-day in the chains...
  - But taking over the browser MAY have only been 1-day:
    Take patch, derive exploit. (We just don't know...)